

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-004037

(43)Date of publication of application : 09.01.1990

(51)Int.Cl.

H04L 9/06

H04L 9/14

(21)Application number : 63-152270

(71)Applicant : CANON INC

(22)Date of filing : 22.06.1988

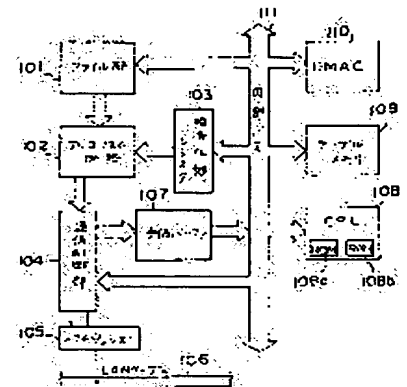
(72)Inventor : ARAKAWA TADASHI

(54) LAN ENCIPHERMENT SYSTEM

(57)Abstract:

PURPOSE: To increase the security effect of information by enciphering a file from a file server and outputting it onto a LAN by means of an encipherment corresponding to a user to give a file access request.

CONSTITUTION: When a file access packet from an arbitrary terminal on the LAN is inputted through a driver/receiver 105 and a communication control 104 to a receiving buffer 107, a CPU 108 confirms a file name. Next, a user identifier is known, and an access right to the file name is checked. When the check is passed, an enciphering key to be uniquely decided by the user ID is set to an enciphering key register 103. There, the CPU 108 starts a file transfer. The file is enciphered through an algorithm circuit 102, made into a packet by the communication control 104 and made to flow onto a LAN cable 106 by adding the address of the opposite party to it.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

Japanese Publication for Unexamined Patent Application
No. 4037/1990 (*Tokukaihei* 2-4037)

A. Relevance of the Above-identified Document

 This document has relevance to claims 1, 17, and 18
of the present application.

B. Translation of the Relevant Passages of the Document

 See the attached English Abstract.

THIS PAGE BLANK (USPTO)

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平2-4037

⑮ Int. Cl.⁵

識別記号

庁内整理番号

⑬ 公開 平成2年(1990)1月9日

H 04 L 9/06
9/14

7240-5K H 04 L 9/02 Z
審査請求 未請求 請求項の数 1 (全5頁)

⑭ 発明の名称 LAN暗号化方式

⑯ 特 願 昭63-152270

⑰ 出 願 昭63(1988)6月22日

⑱ 発 明 者 荒 川 忠 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
⑲ 出 願 人 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
⑳ 代 理 人 弁理士 大塚 康德 外1名

(57) 【要約】

〔目的〕 ファイルアクセス要求を出したユーザに対応する暗号化によつて、ファイルサーバからファイルを暗号化してLAN上へ出力することにより、情報のセキュリティ効果を高める。

〔構成〕 LAN上の任意端末からのファイルアクセスパケットがドライバ／レシーバ105、通信制御104を通り、受信バッファ107に入ると、CPU108はファイル名を確認する。次に、ユーザ識別子を知り、ファイル名へのアクセス権をチェックする。チェックがパスすると、ユーザIDにて一意的に決まる暗号化鍵を暗号化鍵レジスタ103へセットする。そこで、CPU108はファイル転送を開始する。ファイルはアルゴリズム回路102を通つて暗号化され、通信制御104でパケット化され、相手アドレスを付加してLANケーブル106上へ流される。

【LAN 暗号化 方式 ファイル アクセス 要求 出し 利用者 対応 暗号化 ファイル サーバ ファイル 出力 情報 安全 効果 高める 任意 端末 パケット ドライバ レシーバ 通信 制御 通り 受信 バッファ 入り CPU ファイル 名 確認 利用者 識別 子 知り アクセス権 チェック パス 利用者 ID 一意的 暗号化鍵 レジスタ セット ファイル 転送 開始 アルゴリズム 回路 相手 アドレス 付加 LAN ケーブル】

(2)

1

2

【特許請求の範囲】

ファイルサーバにおいて暗号化を行うLAN暗号化方式であつて、

ファイルアクセス情報内のユーザ識別子を識別する識別手段と、

該ユーザ識別子に対応して所定の暗号化鍵を記憶する暗号化鍵記憶手段と、

該暗号化鍵記憶手段から読み出された暗号化鍵に対応して暗号化を行う暗号化手段とを備え、LANからのファイルアクセス要求に対して、前記ファイルサーバは、該
10
ファイルアクセス要求を出したユーザに対応する暗号化により、ファイルをLAN上へ出力することを特徴とするLAN暗号化方式。

(3)

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平2-4037

⑬ Int. Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)1月9日

H 04 L 9/06
9/147240-5K H 04 L 9/02 Z
審査請求 未請求 請求項の数 1 (全5頁)

⑮ 発明の名称 LAN暗号化方式

⑯ 特 願 昭63-152270

⑰ 出 願 昭63(1988)6月22日

⑱ 発 明 者 荒 川 忠 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
 ⑲ 出 願 人 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
 ⑳ 代 理 人 弁理士 大塚 康徳 外1名

明 細 書

暗号化方式。

1. 発明の名称

LAN暗号化方式

2. 特許請求の範囲

ファイルサーバにおいて暗号化を行うLAN
暗号化方式であつて、

ファイルアクセス情報内のユーザ識別子を識別
する識別手段と、

該ユーザ識別子に対応して所定の暗号化鍵を
記憶する暗号化鍵記憶手段と、

該暗号化鍵記憶手段から読み出された暗号化鍵
に対応して暗号化を行う暗号化手段とを備え、

LANからのファイルアクセス要求に対して、
前記ファイルサーバは、該ファイルアクセス要求
を出したユーザに対応する暗号化により、ファイ
ルをLAN上へ出力することを特徴とするLAN

(4)

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明はLAN（ローカルエリアネットワーク）の暗号化方式に関するものである。

〔従来の技術〕

LANにおいては、高速の共通通信路上に位置する各装置に媒体アクセス制御機能が分散され、各装置は対等の関係にあつて、同報機能、任意の装置間通信、通信路上の各種資源の共有等が実現されている。更に、データファイルも基本的には共有であるが、そのデータファイルが、例えば学生の成績、病院のカルテ、企業の経理情報・人事情報・マル秘文書等のいわゆる機密情報・個人情報に対しては、セキュリティの確保がなされている。

これが、ユーザ識別子（ID：認識ラベル）の

場所で行われ、その後データベースの形でLAN上に位置するファイルサーバに供給され、端末ユーザに開放される。

本発明は、前記従来の欠点及び上記の点に鑑み、ファイルサーバからの出力時にデータが暗号化されるLAN暗号化方式を提供する。

又、本発明は、ファイルアクセスユーザは各ユーザ毎の専用復号化鍵を所有することを可能としたものである。

〔問題点を解決するための手段〕

この課題を解決するために、本発明のLAN暗号化方式は、ファイルサーバにおいて暗号化を行うLAN暗号化方式であつて、

ファイルアクセス情報内のユーザ識別子を識別する識別手段と、該ユーザ識別子に対応して所定の暗号化鍵を記憶する暗号化鍵記憶手段と、

特開平2-4037(2)

導入及びデータファイル等のアクセスレベルの設定とグループ化とによるアクセス権の制限である。この方式により不正アクセスの未然防止がなされ、現在のLANシステムでは一般的に採用されている。

〔発明が解決しようとする課題〕

しかしながら、共通通信路を流れる信号を直に盗聴することはどこでも可能なため、データ盗用の完全なる防止をアクセス権の制限だけで行うには無理がある。従つて、共通通信路上の信号が暗号化されることが、セキュリティ対策上最良といえる。しかし、暗号化アルゴリズムと暗号化鍵／復号化鍵をLANユーザに簡単に提供できるLAN暗号化方式は存在しなかった。

又、機密情報、マル秘情報等セキュリティの強化を要する情報の更新の多くはLAN以外の

該暗号化鍵記憶手段から読み出された暗号化鍵に対応して暗号化を行う暗号化手段とを備える。

〔作用〕

かかる構成において、LANからのファイルアクセス要求に対して、前記ファイルサーバは、該ファイルアクセス要求を出したユーザに対応する暗号化により、ファイルをLAN上へ出力する。

〔実施例〕

第4図は本実施例のシステム構成図であり、本実施例におけるファイルサーバの位置付けを表している。同図において、401-1～401-nは端末を表わし、402はファイルサーバ（FS）、403はファイルサーバ更新用端末、404はゲートウェイ（GW）である。端末401-1～401-n、ファイルサーバ402、

(5)

特開平2-4037 (3)

ゲートウェイ404はLAN407で結ばれている。405は公衆網、406はLAN407外の端末である。ファイルサーバ402はLAN407内の端末401-1〜401-nからアクセスされるとともに、ゲートウェイ404を介して公衆網に接続された端末406からもアクセスされることを示している。

第1図はファイルサーバ402内のハードウェアブロック図の1例を示したものである。図中、101はデータベースとしてのファイル部であり、102は暗号化を行うアルゴリズム回路、103は暗号化鍵を格納する暗号化鍵レジスタ、104はパケットの生成・分解等を行う通信制御部、105はドライバ/レシーバであり、LANケーブル106につながる。107は受信バッファ、108は全体を制御するCPU

で処理手順を格納するROM108aと補助記憶用のRAM108bとを有する。109はテーブル情報が格納されるテーブルメモリ、110はDMAコントローラ(DMAC)、111は内部バスである。

この構成における本実施例の動作を、第2図に示すフローチャートに従って説明する。

LAN上の任意の端末からのファイルアクセスパケットがドライバ/レシーバ105、通信制御部104を通り、受信バッファ107に入ると、CPU108はパケットを解析し、ステップS1でファイルアクセスパケットであることを確認するとともにアクセス対策となるファイル名を確認する。次にステップS2でパケットのユーザ識別子フィールドからユーザ識別子を知り、ステップS3でそのファイル名へのアクセス

権を、ファイルのディレクトリ情報に含まれる属性とユーザ識別子との比較によりチェックする。

チェックがパスしたら、ステップS4でユーザIDにて一意的に決まる暗号化鍵をテーブルメモリ109から入手し、暗号化鍵レジスタ103へセットする。テーブルメモリ109内のユーザ識別子と暗号化鍵の一例を第3図に示す。暗号化鍵レジスタ103の出力はアルゴリズム回路102に入力されており、従ってステップS4にてアルゴリズム回路102はステップS2で確認されたユーザID専用の暗号回路として動作する。

次にCPU108は、ステップS5でDMAC110にそのファイル名のアドレスとバイト長とをセットし、ファイル転送を開始する。ファイル部101のファイル群から出力されたファイル

は、アルゴリズム回路102を通り暗号化され通信制御部104でパケット化され、相手アドレスを付加されてドライバ/レシーバ105を通過してLANケーブル106上へ流れていく。ファイル転送が終了すると、ステップS6からステップS7に進んで、暗号化鍵レジスタ103をリセットしてファイルサーバ402の動作は終了する。このリセット値は暗号化鍵のデフォルト値となり、第3図で示したテーブルに暗号化鍵が記載されていない場合に、用いられる暗号化鍵となる。

LAN上を流れる暗号化された信号は、要求元の端末にて受信される。その端末を操作しているユーザは、ユーザ識別子で決まる自分専用の復号化鍵を用いることにより復号化が可能となる。以上で各ユーザ毎に割付けられた暗号化鍵で暗号化された信号にてファイルサーバからアクセス

(6)

特開平2-4037 (4)

ユーザに要求ファイルが届けられたここになる。

以上説明したように、暗号化鍵とユーザ識別子の対応テーブルをファイルサーバ内に保持することにより、鍵の情報交換のわずらわしさを不用とした簡易な暗号化処理が可能となり、セキュリティの高いLANシステムが構築できるという効果がある。

〔発明の効果〕

本発明により、ファイルサーバからの出力時にデータが暗号化されるLAN暗号化方式を提供できる。

又、ファイルアクセスユーザが各ユーザ毎の専用復号化鍵を所有することが可能となった。

4. 図面の簡単な説明

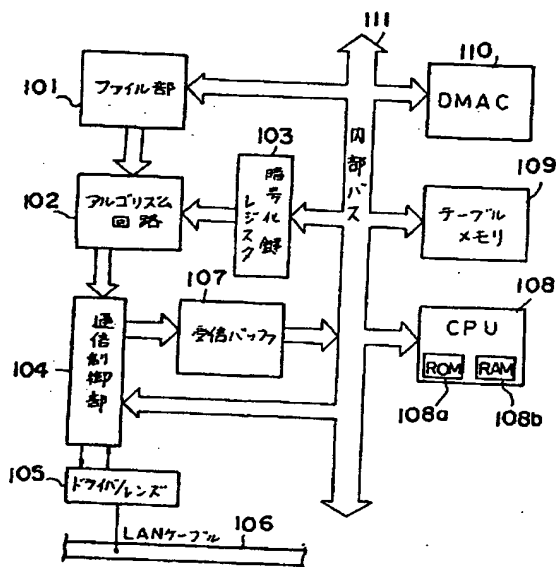
第1図は本実施例の主要部をなすファイナルサーバのハードウェアブロック図、

第2図は本実施例のファイルサーバの動作フローチャート、

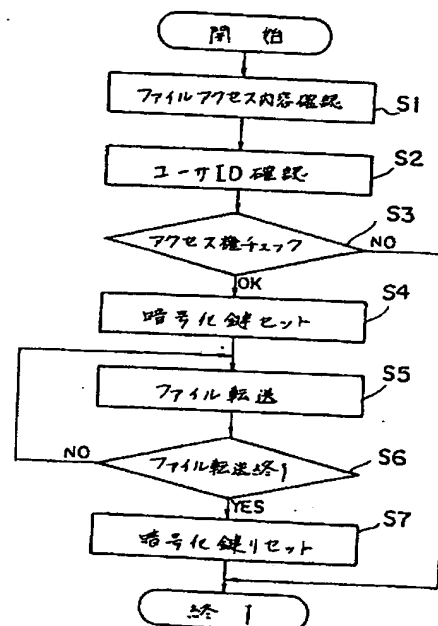
第3図はファイナルサーバ内テーブルメモリのデータ配置を表わす図、

第4図は本実施例のLANシステムの構成図である。

図中、401-1〜401-n、403、406…端末、404…ゲートウェイ、402…ファイルサーバ、405…広域網、407…LAN、101…ファイル部、102…アルゴリズム回路、103…暗号化鍵レジスタ、104…通信制御部、105…レシーバ/ドライバ、106…LANケーブル、107…受信バッファ、108…CPU、108a…ROM、108b…RAM、109…テーブルメモリ、110…DMAC、111…内部バスである。



第1図



第2図

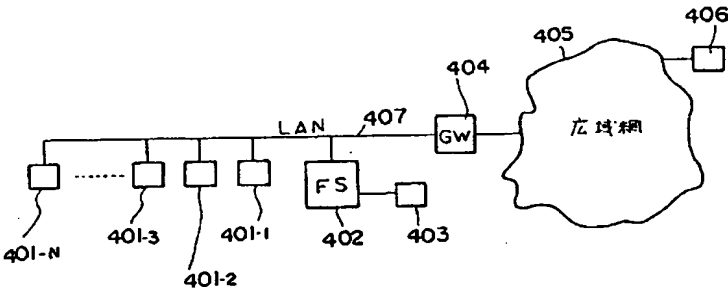
(7)

特開平2-4037 (5)

109

1-710	暗号化鍵
AAA	a b c
BBB	b c d
CCC	c d e
⋮	⋮

第 3 図



第 4 図

THIS PAGE BLANK (USPTO)